CASE STUDY

Closing the Loop: Making Security Everyone's Business with Prioritization & Collaboration

The Challenge

- Maintaining a consolidated, contextualized view of risk posture and priorities across pipelines
- Reducing the alert fatigue and backlog from fragmented tools
- Determining which fixer or team was responsible for implementing a remediation

The Solution

- Prioritize remediation actions based on risk and business context, reduce alert backlog
- Leverage better view of risk profile and priorities to communicate and align with software development teams on where to focus, and why - helping to reverse their security alert fatigue
- Scale remediation operationalization through bulk ticketing in remediation campaigns for findings with a common fix

The Results

- Reduced manual reviews by 80%
- Reduced time spent on prioritization efforts by 70%
- Reduced time spent identifying and assigning fix responsibility by 80%
- Improved number of closed findings by 600% on a monthly basis

Industry Technology

Location Rotterdam, Netherlands

Number of employees 1500

Armis Centrix™ for VIPR Pro – Prioritization and Remediation

Background

Mendix, a Siemens business, is an industry leading low-code application development platform that helps organizations build multi-experience, enterprise grade applications at scale. More than 4,000 organizations in 46 countries use the Mendix low-code platform. An active community of over 300,000 developers has created over 950,000 applications.

The Challenge

As Mendix modernized its application lifecycle and transitioned to the cloud, the security team encountered challenges in:

- Consolidating findings from multiple tools to improve assessment of technology risk
- Identifying high-impact fixes earlier in the software pipeline
- Communicating priorities effectively with engineering teams to improve collaboration and reduce their alert fatigue from the high volume of requests with limited context
- Consistently enabling the "last mile" of remediation - assigning responsibility for the fix to the right owner in their software development teams

The outcome was significant inefficiencies in risk prioritization, and time-consuming, manual efforts to establish which teams and individuals on the engineering team were responsible for remediation fixes and the issuing of individual tickets for issues with a common fix.

As the alert backlog grew, the problem of prioritization and assignment inefficiencies intensified and consumed an increasing amount of time and resources.

"Armis Centrix™ for VIPR Pro – Prioritization and Remediation has positively impacted both the productivity and the efficiency of the security team in identifying risks to the business, as well as how the function of security is integrated into our development processes. The security team can collaborate more closely with development teams responsible for the fix implementation of identified priorities, and improve our overall risk profile."

Frank Baalbergen
CISO, Mendix

The Solution

Mendix deployed the Armis Centrix™ for VIPR Pro – Prioritization and Remediation platform and implemented agentless integration across their pipelines, from the code repository to the cloud environment, in addition to multiple security detection tools for vulnerabilities, code, container and infrastructure security issues.

With consolidated findings, visibility, asset profiling and threat intelligence, the security team gained a much clearer picture of which findings to prioritize based on risk and impact. By understanding how findings were related through asset linking, the security could focus remediation efforts on the earliest point possible in the pipeline.

With a clearer understanding of Mendix's risk profile and priorities in place, security teams could interact more constructively with the engineering teams on where to focus based on clear guidance - counteracting alert fatigue.

In tandem with consolidating and prioritizing tool output, the security team also implemented the platform's predictive assignment for ownership and ticketing integration to minimize manual efforts to identify the fixer, resulting in faster remediation and deeper collaboration between security and software development teams.

Ongoing feedback from software development teams enhanced the accuracy of assignment responsibility, and modifications to the ticketing integrations to accommodate the teams-model preferred by some software development groups, reinforced these collaborations and time to remediation improvements.

In addition, the security team utilized automation for remediation campaigns - bulk ticketing for a set of related findings with a common fix - and for closing tickets for fixed findings.

600% Improved number of closed findings on a monthly basis

80% Reduced time spent identifying and assigning fix responsibility

70% Reduced time spent on prioritization efforts

The Results

The security team experienced significant operational improvements across the remediation lifecycle, and the time consumed by assigning fix responsibility was significantly reduced.

With more detection tools and asset data sources integrated, the team refined prioritization and assignment rules tailored for their environment to build a much clearer and more reliable picture of remediation progress and technology risk.

The ability to facilitate the "last mile" of the remediation process by identifying which team or person can implement the fix both reduced the pressure on the security team to add additional headcount to handle assignments and helped to make security an integral part of the fixer's daily operations.

The combination of operational efficiencies with more accurate and up-to-date reporting has allowed the team to more proactively manage their risk profile. In turn, more automated fix assignment for findings with relatively high urgency allows Mendix to reduce the exposure window, and foster collaboration with software development teams based on clear communication of the relative risk of findings.

ARMIS

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011
www.armis.com